

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

The Apple account "zjoe.mach11@yahoo.com" controlled by
Apple Inc., headquartered at One Apple Park Way, Cupertino,
California, as further described in Attachment A.

Case No. MJ21-059

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty
of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):

The Apple account "zjoe.mach11@yahoo.com" controlled by Apple Inc., headquartered at One Apple Park Way, Cupertino,
California, as further described in Attachment A.

located in the Northern District of California, there is now concealed (identify the
person or describe the property to be seized):

See Attachment A and B for a list of information to be disclosed.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

| | |
|------------------|-----------------------|
| 18 U.S.C. §1343 | Wire Fraud |
| 18 U.S.C. § 1956 | Money Laundering |
| 18 U.S.C. §641 | Theft of public funds |

The application is based on these facts:

- ☒ See Affidavit of Special Agent Andrea Desanto, continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.



Applicant's signature

FBI Special Agent Andrea Desanto

Printed name and title

☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 01/29/2021



Judge's signature

City and state: Seattle, Washington

Michelle L. Peterson, United States Magistrate Judge

Printed name and title

1 evidence of the fraud and may enable investigators to identify the perpetrator.
2 Accordingly, I submit that there is probable cause to believe that the information
3 described in Attachment A contains evidence of violations of Title 18 United States
4 Code, Sections 1343 (wire fraud), 1956 (money laundering), 641 (theft of public funds),
5 371 (conspiracy), and 1028A (aggravated identity theft) as described in Attachment B.

6 4. The information set forth in this affidavit is not intended to detail each and
7 every fact and circumstance of the investigation or all information known to me or the
8 investigative participants. Rather, this affidavit is intended to present the facts relevant to
9 the issue of whether there is probable cause to issue the requested search warrant.

10 5. ***Agent Background and Experience:*** I am currently assigned to the Seattle
11 Field Office. My primary duties include investigating violations of federal law, including
12 but not limited to, Title 18, United States Code, Sections 1343 (wire fraud), 1028A
13 (aggravated identity Theft), 1956 (money laundering), 1957 (transactional money
14 laundering), and conspiracy to commit these offenses. I previously worked on the Cyber
15 squad, where I primarily investigated computer intrusions and other cybercrimes. My
16 experience as an FBI agent includes the investigation of cases involving the use of
17 computers and the Internet to commit crimes. In addition to my experience with
18 cybercrime investigations, I also have experience with financial investigations. I have
19 received formal training on tracing the financial proceeds of crimes. I have applied that
20 training in the context of numerous investigations in which I have reviewed records from
21 financial institutions both in the United States and in foreign jurisdictions, in order to
22 identify the proceeds of criminal offenses under investigation.

23 6. Based on my training and experience, I am familiar with the ways in which
24 individuals involved in fraud schemes use shell e-mail accounts, computers, cellular
25 telephones, Internet Protocol ("IP") addresses, bank accounts, synthetic identities, and
26 counterfeit documents to facilitate fraudulent activity. I have learned that individuals
27 perpetrating computer intrusions and identity theft-related bank fraud and wire fraud
28 schemes employ a number of techniques, either alone or in combination, to further their

1 | illegal activities and to avoid detection by law enforcement. These techniques include:
 2 | utilizing web-based email accounts and other electronic messaging accounts to send,
 3 | receive, store, and obtain personal identifying information, such as dates of birth and
 4 | bank and credit card account numbers and related information; and the use of cloud-
 5 | based accounts to communicate and store information and tools related to the fraud. I
 6 | know that individuals involved in fraud schemes often establish shell e-mail accounts and
 7 | e-mail addresses in fictitious names and/or in the names of third parties in an effort to
 8 | conceal their identities and illicit activities from law enforcement. I know that
 9 | individuals involved in fraud often use virtual private network (“VPN”) accounts and
 10 | Internet hosting services to conceal their true identities and geographical locations from
 11 | law enforcement or other entities.

12 | **JURISDICTION**

13 | 7. This Court has jurisdiction to issue the requested warrant because it is “a
 14 | court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a),
 15 | (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . .
 16 | that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

17 | **STATEMENT OF PROBABLE CAUSE**

18 | **A. Background**

19 | 8. Based on publicly-available information, I know that on March 27, 2020,
 20 | the United States enacted into law the Coronavirus Aid, Relief, and Economic Security
 21 | (CARES) Act. The CARES Act authorized approximately \$2 trillion in aid to American
 22 | workers, families, and businesses to mitigate the economic consequences of the COVID-
 23 | 19 pandemic. The CARES Act funded and authorized each state to administer new
 24 | unemployment benefits. These benefits include: (1) Federal Pandemic Unemployment
 25 | Compensation (FPUC), which provides an additional benefit of \$600 per week per
 26 | unemployed worker; (2) Pandemic Unemployment Assistance (PUA), which extends
 27 | benefits to self-employed persons, independent contractors, and others; and (3) Pandemic
 28 |

1 Emergency Unemployment Assistance (PEUC), which extends benefits for an additional
2 13 weeks after regular unemployment benefits are exhausted. All of these programs will
3 be referenced herein as “CARES Act benefits.” The CARES Act allows an unemployed
4 worker to obtain back benefits retroactive to the date on which the applicant was affected
5 by COVID 19, which, under program rules, may be as early as February 2, 2020.

6 9. The Washington Employment Security Department (ESD) is the
7 component of the State of Washington responsible for administering unemployment
8 benefits, including CARES Act benefits. Applicants apply for ESD-administered
9 benefits using ESD’s Secure Access Washington (SAW) web portal. To submit an
10 application, the applicant must enter his or her personal identifying information
11 (including name, date of birth, and Social Security number). ESD checks this
12 information against its database of Washington residents. If ESD confirms that the
13 information matches the personal identifying information of a person in ESD’s records,
14 ESD will pay out benefits via wire (ACH) transfer to an account identified by the
15 applicant.

16 10. Prior to March 2020, before paying unemployment benefits to a worker,
17 ESD generally required the worker’s employer to provide confirmation that the employee
18 had ceased working for the employer, and further, that the circumstances surrounding the
19 termination rendered the employee eligible for unemployment assistance. However, in or
20 about March 2020, as a result of changes in eligibility resulting from the CARES Act,
21 and in an effort to distribute funds as quickly as possible, ESD stopped requiring
22 employer verification before it paid claims.

23 **B. Overview of Investigation**

24 11. Beginning on or around April 20, 2020, law enforcement officials began
25 receiving complaints from employers about potentially fraudulent unemployment claims.
26 The employers reported that they had received notices from ESD indicating that persons
27 still under their employ had filed unemployment claims. For example, on or about April
28 20, 2020, the Seattle Fire Department (SFD) notified the U.S. Attorney’s Office for the

1 Western District of Washington that claims had been filed in the names of multiple
2 firefighters who were actively employed by SFD. SFD reported that it had interviewed
3 the firefighters, who had denied any involvement in the claims. Other employers,
4 including Microsoft Corporation, the City of Bellingham, Zulily, and Seattle Yacht Club
5 submitted similar complaints.

6 12. Roughly around that same time, numerous other agencies, including the
7 Federal Bureau of Investigation, the Social Security Administration Office of Inspector
8 General, the United States Secret Service, the Department of Labor Office of the
9 Inspector General, the United States Postal Inspection Service, and Internal Revenue
10 Service Criminal Investigation, joined the investigation. Agents from these agencies,
11 including myself, have reviewed voluminous financial records and databases reflecting
12 the fraudulent transactions and have conducted dozens of interviews.

13 13. The total amount of fraudulent claims paid out by ESD is currently
14 unknown. However, ESD's Commissioner, Suzi LeVine, has publicly stated ESD has
15 paid out in excess of \$600 million in fraudulent claims.

16 **C. Role of Gmail Accounts in the Fraud**

17 14. As discussed above, applicants apply for ESD benefits using ESD's secure
18 web portal, SAW. I have had communications with ESD employees and have also
19 visited the SAW portal. I have learned that, when an applicant applies for benefits
20 through SAW, the applicant is required to provide an email address. After the initial
21 application is submitted, ESD sends an authentication email to the address the user
22 provided. To continue the application process, the user must then access the email
23 account and click on an activation link. The user may then return to the SAW portal and
24 complete the application process. By necessity then, each email account associated with
25 a fraudulent claim must have been accessed, as part of the fraud, by a participant in the
26 fraud scheme.

27 15. ESD provided the government with data identifying the email accounts the
28 criminals used when submitting their fraudulent claims. The data indicate that the

1 criminals used thousands of different email accounts for this purpose, including accounts
2 operated by Google.

3 16. For many of these Google email accounts, perpetrators took advantage of a
4 particular feature of Google email accounts that allowed them to submit multiple
5 fraudulent claims from a single Google email account without ESD detecting that a single
6 email address was being used repeatedly. This feature is that, in routing emails to an
7 email box, Google disregards periods in the email address, meaning that the email
8 address “john.doe@gmail.com” and “johndoe@gmail.com” will resolve to the same
9 Google email account, even though ESD identifies them as two different accounts. Two
10 email addresses like these that are distinguished only by periods are known as “Google
11 variants” or “dot variants.” I know from my training and experience that criminals
12 sometimes take advantage of this feature to make it appear that emails are originating
13 from multiple accounts, when in fact they originate from the same account. This reduces
14 the number of email accounts that a criminal must open and monitor while perpetrating a
15 fraud, while avoiding fraud alerts that may be triggered when multiple claims originate
16 from the same account.

17 **D. Use of the MillerPepe2020@gmail.com Account**

18 17. The database that ESD provided to the government identified the email
19 address used to activate each fraudulent claim. Investigators grouped these accounts by
20 email provider, and found that Google-hosted email accounts were used to activate over
21 30,000 fraudulent ESD claims.

22 18. Investigators then analyzed the database to identify Gmail accounts that
23 criminals used to submit multiple claims using the Google dot variant method discussed
24 above. Investigators identified over 1,200 dot variant accounts used to submit multiple
25 claims to ESD, and further identified 32 accounts that were used to submit particularly
26 large volumes of claims. Among these accounts was **millерpepe2020@gmail.com**.

27 19. On June 19, 2020, the government applied for, and the Honorable Paula L.
28 McCandlis issued, an order pursuant to 18 U.S.C. § 2703(d), directing Google to produce

1 non-content material associated with the 32 accounts described above. The order
2 required Google to identify, for each account, the recovery information for the account,
3 and other Google accounts linked to these accounts by common recovery information,
4 cookies, or other means.

5 20. According to ESD's claims database, criminals used over 200 dot variants
6 of **millerpepe2020@gmail.com**¹ to claim ESD benefits in excess of \$1 million.
7 Moreover, Google's 2703(d) order response confirmed that **millerpepe2020@gmail.com**
8 received confirmation emails from ESD for the fraudulent claims filed using those
9 accounts and their email variants. The response also indicated that the account had
10 received a large volume of emails from unemployment agencies for the states of New
11 York and Maine.

12 21. Google's 2703(d) order response indicated that the
13 **millerpepe2020@gmail.com** account had been created on April 6, 2020, which was just
14 10 days after the CARES Act was enacted. Google's response also revealed that the
15 account was created using an IP address that an open source WHOIS search shows is a
16 Nigeria-based IP address.

17 22. The 2703(d) order also required Google to identify the recovery email
18 accounts for the subject accounts. Based on my training and experience, I know that a
19 recovery email account is an additional email address supplied by the user that is used by
20 the email provider to communicate with the user outside of the account itself, such as to
21 help the user if the user is having trouble signing into their account (e.g., by sending a
22 password reminder or password reset link), or to alert the user to any unusual activity
23 involving the user's email address. When one account is listed as the recovery account
24 for another account, this connection strongly suggests common ownership between the
25 two accounts. Recovery accounts often contain information about the user of the linked
26 account, which allows investigators to determine the true identity of person operating that

27
28 ¹E.g., mil.l.er.p.epe2020@gmail.com, m.ille.r.p.e2020@gmail.com, and mill.e.rpe.pe2020@gmail.com.

1 original account. Google's 2703(d) order response revealed that the recovery email
2 account for **millerpepe2020@gmail.com** was **frankmorris004@gmail.com**. In
3 addition, Google's 2703(d) order response revealed that **frankmorris004@gmail.com**
4 and **millerpepe2020@gmail.com** are linked by cookies, signifying that both
5 **frankmorris004@gmail.com** and **millerpepe2020@gmail.com** have been accessed
6 from the same computer.

7 23. Furthermore, Google's 2703(d) order response identified all Gmail
8 accounts that also use account **frankmorris004@gmail.com** as their secondary email
9 account. Among those Gmail accounts was account **machjoe2020@gmail.com**, which
10 has a similar username to the TARGET ACCOUNT Apple ID **zjoe.mach11@yahoo.com**
11 and to other usernames further discussed below. I know from my training and experience
12 that persons engaging in fraud over the internet often use multiple email accounts with
13 closely-related names to conduct different parts of their fraud schemes.

14 24. The 2703(d) order also required Google to identify the recovery telephone
15 number associated with the listed accounts, and to identify any other accounts that share
16 the same recovery number. Like a recovery email address, a recovery telephone number
17 is a means to contact an account user outside of the account itself (e.g., for purposes of
18 two-factor authentication or password recovery). Google's response to the 2703(d) order
19 indicated that the recovery telephone number for **millerpepe2020@gmail.com** is +234
20 802 900 3211 (the "3211 SMS Number"). The "234" prefix is the country code assigned
21 to Nigeria.

22 25. In addition, Google's 2703(d) response indicated that several other email
23 accounts – **millerpeperay2020@gmail.com**, **peperay2016@gmail.com**, and
24 **newpeperay@gmail.com** – *both*: (1) use the 3211 SMS Number as a recovery phone
25 number; *and* (2) were linked by cookies with **millerpepe2020@gmail.com**. Of note,
26 each of these account names contains a variation of the name "Pepe Ray," which is
27 discussed further below.
28

26. On November 30, 2020, the Honorable Mary Alice Theiler issued a search warrant to Google for, *inter alia*, **millerpepe2020@gmail.com**, **frankmorris004@gmail.com**, **millerpeperay2020@gmail.com**, **peperay2016@gmail.com**, and **newpeperay@gmail.com** (“November 2020 Google search warrant”).

27. Google responded to the search warrant on approximately January 19, 2021. The contents of **millerpepe2020@gmail.com** included a large volume of emails from ESD, as well as from the unemployment agencies from the states of New York, Maine, Pennsylvania, and Idaho. In addition, the account contained many emails from the Kansas Department of Labor indicating that the account had been used to file numerous claims in Kansas as recently as November 2020. The account also contained numerous emails from Green Dot and MOVO, which are payment systems that I know were used to collect and transfer a large share of the claims that were filed with ESD using the **millerpepe2020@gmail.com** account. Agents are continuing to review the responsive material, some of which is discussed below.

E. Investigation of the 3211 SMS Number and “Pepe Ray”

28. As noted above, the 3211 SMS Number is the recovery number for **millerpepe202@gmail.com**. Based on open source research, investigators determined that the 3211 SMS Number is associated with a WhatsApp account. WhatsApp is a multiplatform messaging and calling app. Investigators requested subscriber information for the account from WhatsApp. WhatsApp’s records indicated that the account was opened in April 2013, and remains active. The name associated with the WhatsApp account is “Pepe Ray.” The records further indicated that the phone used to access the WhatsApp account is an Apple iPhone 11 Pro.

29. Based on open source research, investigators also identified a Snapchat (another multiplatform messaging app) account associated with the 3211 SMS Number. According to the account’s public-facing profile, the user ID for that account is “iampeperay,” and the username is “Pepe Ray.” Investigators requested subscriber

records for the account from Snapchat. Snapchat's response indicated that the recovery email for the account is **peperay@yahoo.com**. Notably, information provided by Google in response to the November 2020 Google search warrant revealed that **peperay@yahoo.com** was saved as a contact in the **frankmorris004@gmail.com** account. Furthermore, Google's response to the November 2020 search warrant revealed that **frankmorris004@gmail.com** had received multiple emails from Yahoo with an email sign-in verification code for account **peperay@yahoo.com**. Based on my training and experience, this indicates that account **frankmorris004@gmail.com** is likely a recovery email for account **peperay@yahoo.com**, and the two accounts are likely controlled by the same individual.

30. In addition, open source research revealed that an Instagram account with the screen name "Iampeperay" is also associated with the 3211 SMS Number. Instagram is a photo and video sharing social networking service owned by Facebook, Inc. Agents obtained subscriber records from Instagram, which indicated that the name of the subscriber is "Pepe Ray." Also according to these records, the email address associated with the Instagram account is **joe.mach@yahoo.com**, which, like **machjoe2020@gmail.com**, discussed above, is similar to the moniker associated with the TARGET ACCOUNT Apple ID (i.e., **zjoe.mach11@yahoo.com**). In addition, the address **joe.mach11@yahoo.com** was also saved as a contact in **frankmorris004@gmail.com**.

H. The Target Apple Account

31. As noted above, WhatsApp records indicated that an Apple iPhone 11 Pro was being used to access the WhatsApp account associated with the 3211 SMS Number. Accordingly, investigators requested information from Apple about any Apple account associated with the 3211 SMS Number.

32. Apple's response to the government's request indicated that the 3211 SMS Number is associated with an Apple account with the Apple ID "**zjoe.mach11@yahoo.com**" (the TARGET ACCOUNT). Specifically, the 3211 SMS

1 Number is the number used for two-factor authentication and to send and receive SMS,
2 Apple iMessages, and FaceTime calls for the TARGET ACCOUNT. Apple's response
3 indicated that the TARGET ACCOUNT was opened on January 22, 2016, and remains
4 active. The response discloses that the most recent device registered on the TARGET
5 ACCOUNT is an iPhone 11 Pro, which is consistent with the information provided in
6 WhatsApp's response for the account with username "Pepe Ray," discussed above.

7 33. Google's 2703(d) order response also indicated that
8 **millerpepe2020@gmail.com** had been accessed using two Trifone brand, Passion Plus
9 model, devices. Open source research indicates that Trifone phones are a Nigerian phone
10 brand. Based on my training and experience, criminals perpetrating frauds use multiple
11 digital devices in order to conceal their true identity and evidence of their crime.

12 34. Apple's response also disclosed that the TARGET ACCOUNT was
13 registered using the IP address 197.210.173.100. According to an open source WHOIS
14 search, the IP address used to register the account originates from Lagos, Nigeria.
15 However, when registering the account with Apple, the subscriber provided the name
16 "Alina Prussky" and claimed to be a resident of Toronto, Canada. I know from my
17 training and experience that persons who commit crime over the internet often use
18 fictitious names and locations to disguise their identities.

19 35. In response to the request, Apple further revealed that the email account
20 that was used to verify the Apple account was **frankmorris004@gmail.com**, which, as
21 discussed above, is also the same recovery email address for account
22 **millerpepe2020@gmail.com** – the account created merely 10 days after the enactment of
23 the CARES Act and used to submit fraudulent claims to ESD as well as unemployment
24 benefits agencies in New York, Maine, Pennsylvania, Idaho and Kansas.

25 36. Based on the information set forth above, it is highly probable that the user
26 of the TARGET ACCOUNT is also the user of **millerpepe2020@gmail.com**. Therefore,
27 probable cause exists to believe the account will contain evidence of the crimes under
28

1 investigation, including but not limited to the identity of the person who submitted the
2 fraudulent claims.

3 **BACKGROUND CONCERNING APPLE**²

4 37. Apple is a United States company that produces the iPhone, iPad, and iPod
5 Touch, all of which use the iOS operating system, and desktop and laptop computers
6 based on the Mac OS operating system.

7 38. Apple provides a variety of services that can be accessed from Apple
8 devices or, in some cases, other devices via web browsers or mobile and desktop
9 applications (“apps”). Following are some of the services Apple provides that are
10 relevant here:

11 a. iCloud is a cloud storage and cloud computing service from Apple
12 that allows its users to interact with Apple’s servers to utilize iCloud-connected services
13 to create, store, access, share, and synchronize data on Apple devices or via icloud.com
14 on any Internet-connected device.

15 b. iCloud Backup allows users to create a backup of their device data.

16 c. iCloud Photo Library and My Photo Stream can be used to store and
17 manage images and videos taken from Apple devices, and iCloud Photo Sharing allows
18 the user to share those images and videos with other Apple subscribers.

19 d. iCloud Drive can be used to store presentations, spreadsheets, and
20 other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize
21 bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple
22 devices.

23 e. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote,
24 and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets,
25 and presentations. iCloud Keychain enables a user to keep website username and
26 passwords, credit card information, and Wi-Fi network information synchronized across
27 multiple Apple devices.

28 ² The information in this section is based on information published by Apple on its website, including, but
not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available
at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Create and start using an Apple ID,”
available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What
does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at
https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at
<https://support.apple.com/kb/PH26502>.

1 f. Game Center, Apple's social gaming network, allows users of Apple
2 devices to play and share games with each other.

3 g. Find My iPhone allows owners of Apple devices to remotely
4 identify and track the location of, display a message on, and wipe the contents of those
5 devices. Find My Friends allows owners of Apple devices to share locations.

6 h. Location Services allows apps and websites to use information from
7 cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to
8 determine a user's approximate location.

9 i. App Store and iTunes Store are used to purchase and download
10 digital content. iOS apps can be purchased and downloaded through App Store on iOS
11 devices, or through iTunes Store on desktop and laptop computers running either
12 Microsoft Windows or Mac OS. Additional digital content, including music, movies, and
13 television shows, can be purchased through iTunes Store on iOS devices and on desktop
14 and laptop computers running either Microsoft Windows or Mac OS.

15 39. Apple services are accessed through the use of an "Apple ID," an account
16 created during the setup of an Apple device or through the iTunes or iCloud services.
17 The account identifier for an Apple ID is an email address, provided by the user. Users
18 can submit an Apple-provided email address (often ending in @icloud.com, @me.com,
19 or @mac.com) or an email address associated with a third-party email provider (such as
20 Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services
21 (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to
22 a "verification email" sent by Apple to that "primary" email address. Additional email
23 addresses ("alternate," "rescue," and "notification" email addresses) can also be
24 associated with an Apple ID by the user. A single Apple ID can be linked to multiple
25 Apple services and devices, serving as a central authentication and syncing mechanism.

26 40. Apple captures information associated with the creation and use of an
27 Apple ID. During the creation of an Apple ID, the user must provide basic personal
28 information including the user's full name, physical address, and telephone numbers.
The user may also provide means of payment for products offered by Apple. The
subscriber information and password associated with an Apple ID can be changed by the
user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition,

1 Apple captures the date on which the account was created, the length of service, records
2 of log-in times and durations, the types of service utilized, the status of the account
3 (including whether the account is inactive or closed), the methods used to connect to and
4 utilize the account, the Internet Protocol address (“IP address”) used to register and
5 access the account, and other log files that reflect usage of the account.

6 41. Additional information is captured by Apple in connection with the use of
7 an Apple ID to access certain services. For example, Apple maintains connection logs
8 with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes
9 Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on
10 Apple’s website. Apple also maintains records reflecting a user’s app purchases from
11 App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for
12 iMessage, and “mail logs” for activity over an Apple-provided email account. Records
13 relating to the use of the Find My iPhone service, including connection logs and requests
14 to remotely lock or erase a device, are also maintained by Apple.

15 42. Apple also maintains information about the devices associated with an
16 Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains
17 the user’s IP address and identifiers such as the Integrated Circuit Card ID number
18 (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone
19 number of a user’s iPhone is linked to an Apple ID when the user signs into FaceTime or
20 iMessage. Apple also may maintain records of other device identifiers, including the
21 Media Access Control address (“MAC address”), the unique device identifier (“UDID”),
22 and the serial number. In addition, information about a user’s computer is captured when
23 iTunes is used on that computer to play content associated with an Apple ID, and
24 information about a user’s web browser may be captured when used to access services
25 through icloud.com and apple.com. Apple also retains records related to communications
26 between users and Apple customer service, including communications regarding a
27 particular Apple device or service, and the repair history for a device.

43. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

44. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

45. In addition, the user's account activity, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has

1 unique hardware and software identifiers, and because every device that connects to the
2 Internet must use an IP address, IP address and device identifier information can help to
3 identify which computers or other devices were used to access the account. Such
4 information also allows investigators to understand the geographic and chronological
5 context of access, use, and events relating to the crime under investigation.

6 46. In this case, there is probable cause to believe that the user of the TARGET
7 ACCOUNT is the same person as, or is closely associated with, the person who
8 submitted fraudulent claims to ESD using the email address
9 **millerpepe2020@gmail.com**. The contents of the Apple account and associated material
10 may provide information about the identity of this person, as well as evidence of the
11 crime. Based on my training and experience, instant messages, emails, voicemails,
12 photos, videos, and documents are often created and used in furtherance of criminal
13 activity, including to communicate and facilitate the offenses under investigation.

14 47. Account activity may also provide relevant insight into the account owner's
15 state of mind as it relates to the offenses under investigation. For example, information
16 on the account may indicate the owner's motive and intent to commit a crime (e.g.,
17 information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting
18 account information in an effort to conceal evidence from law enforcement).

19 48. Therefore, Apple's servers are likely to contain stored electronic
20 communications and information concerning subscribers and their use of Apple's
21 services. In my training and experience, such information may constitute evidence of the
22 crimes under investigation including information that can be used to identify the
23 account's user or users.

24 **REQUEST FOR NONDISCLOSURE AND SEALING**

25 49. The government requests, pursuant to the preclusion of notice provisions of
26 Title 18, United States Code, Section 2705(b), that Apple be ordered not to notify any
27 person (including the subscriber or customer to which the materials relate) of the
28

1 | existence of this warrant for such period as the Court deems appropriate. In this case,
2 | such an order is appropriate because the search warrant relates to an ongoing criminal
3 | investigation and disclosure would provide the targets with information about the
4 | government's investigation that could be used to frustrate further investigative efforts.

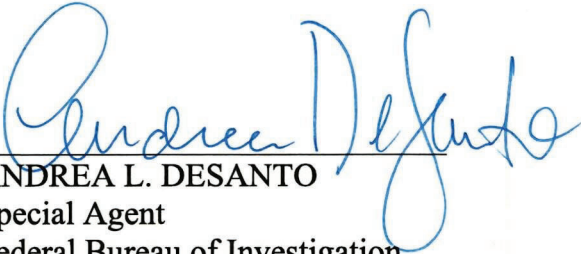
5 | 50. I further request that the Court order that all papers in support of this
6 | application, including the affidavit and search warrant, be sealed until further order of the
7 | Court. These documents discuss an ongoing criminal investigation that is neither public
8 | nor known to all of the targets of the investigation. There is good cause to seal these
9 | documents because their premature disclosure may give the subjects an opportunity to
10 | flee from prosecution, dissipate assets, destroy or tamper with evidence, change patterns
11 | of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

12 | 51. For these reasons, I am requesting that the Court issue an Order sealing the
13 | search warrant, search warrant return, application and affidavit for the search warrant,
14 | and all attachments until the earliest of the following: (a) two weeks following the
15 | appearance of any criminal defendant in the Western District of Washington on a
16 | charging document in a matter for which the warrants were issued; (b) two weeks
17 | following the closure of the investigation for which the warrants were issued; or (c)
18 | sixteen months following issuance of the warrant, unless the Court, upon motion of the
19 | government for good cause, orders an extension of that Order.

20 | CONCLUSION

21 | 52. Based on the foregoing, I believe there is probable cause to believe that
22 | evidence, instrumentalities, contraband, and/or fruits of violations of Title 18, United
23 | States Code, Sections 1343 (wire fraud), 1956 (money laundering), 641 (theft of public
24 | funds), 371 (conspiracy), and 1028A (aggravated identity theft) will be found in the
25 | TARGET ACCOUNT. I therefore request that the Court issue warrants authorizing a
26 | search of the TARGET ACCOUNT, for the items more fully described in Attachment B
27 | hereto, incorporated herein by reference, and the seizure of any such items found therein.
28 |

1 53. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer
2 is not required for the service or execution of this warrant. The government will execute
3 this warrant by serving the warrant on Apple. Because the warrant will be served on
4 Apple, who will then compile the requested records at a time convenient to it, reasonable
5 cause exists to permit the execution of the requested warrant at any time in the day or
6 night.

7
8
9 
10 ANDREA L. DESANTO
11 Special Agent
12 Federal Bureau of Investigation

13 The above-named agent provided a sworn statement attesting to the truth of the contents
14 of the foregoing affidavit by telephone on the 29th day of January, 2021.

15 
16 MICHELLE L. PETERSON
17 United States Magistrate Judge
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A

Property to Be Searched

This warrant applies to the electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the Apple account with the Apple ID **zjoe.mach11@yahoo.com** (the “TARGET ACCOUNT”) as well as all other subscriber and log records associated with the TARGET ACCOUNT, which are located at premises owned, maintained, controlled or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on January 14, 2021, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

I. Material to be Produced by Apple

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from January 22, 2016 to the present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

1 d. The contents of all instant messages associated with the account for the
2 period January 22, 2016 to the present, including stored or preserved copies of instant
3 messages (including iMessages, SMS messages, and MMS messages) sent to and from
4 the account (including all draft and deleted messages), the source and destination account
5 or phone number associated with each instant message, the date and time at which each
6 instant message was sent, the size and length of each instant message, the actual IP
7 addresses of the sender and the recipient of each instant message, and the media, if any,
8 attached to each instant message;

9 e. The contents of all files and other records stored on iCloud, including all
10 iOS device backups, all Apple and third-party app data, all files and other records related
11 to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud
12 Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and
13 bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes,
14 reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

15 f. All activity, connection, and transactional logs for the account (with
16 associated IP addresses including source port numbers), including FaceTime call
17 invitation logs, messaging and query logs (including iMessage, SMS, and MMS
18 messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases,
19 downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs,
20 sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My
21 Friends logs, logs associated with web-based access of Apple services (including all
22 associated identifiers), and logs associated with iOS device purchase, activation, and
23 upgrades;

24 g. All records and information regarding locations where the account or
25 devices associated with the account were accessed, including all data stored in connection
26 with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

27 h. All records pertaining to the types of service used;

28 i. All records pertaining to communications between Apple and any person
regarding the account, including contacts with support services and records of actions
taken; and

j. All files, keys, or other information necessary to decrypt any data produced
in an encrypted form, when available to Apple (including, but not limited to, the
keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14
days of issuance of this warrant.

II. Material to be seized by the government

Upon receipt of the information described in Section I, the government may seize the following material that constitutes evidence and instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud), 1956 (money laundering), 641 (theft of public funds), 371 (conspiracy), and 1028A (aggravated identity theft) for the TARGET ACCOUNT:

- a. Records and information referring or relating to unemployment benefits;
- b. Records and information relating to the laundering of criminal proceeds, the creation and maintenance of financial accounts, financial transfers and transactions, the possession of monetary instruments, and the disbursement of funds;
- c. Records and information relating to stolen personally identifiable information;
- d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner;
- e. Records and information that serves to identify any person who uses or accesses or who exercises in any way any dominion or control over the TARGET ACCOUNT;
- f. Records and information that may reveal the current or past location of the account users;
- g. Records and information that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts;
- h. Records and information relating to the subscriber's state of mind as it relates to the crimes under investigation.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to

1 this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the
2 custody and control of attorneys for the government and their support staff for their
3 independent review.
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT
TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature